DII.COE.Final.HP1020.SAM

Defense Information Infrastructure (DII)

Common Operating Environment (COE)

System Administrator's Manual (SAM) for SATAN, version 1.0.0.2

Document Version 1.0.0.2

18 July 1997

Prepared for:

Defense Information Systems Agency

Prepared by:

NRaD
San Diego, CA

Table of Contents

This page intentionally left blank.

1. Scope

1.1 Identification

This System Administrator's Manual (SAM) document is for SATAN (segprefix SATAN) Version 1.0.0.2 for the HP 10.20 Platform. It provides system administrators specific guidance to support COE system and software installation and maintenance.

1.2 System Overview

This version of SATAN (Security Administrator Tool for Analyzing Networks) remotely probes systems via the network and stores its findings in a database.

System configuration variables and command line options can be found in Appendix A.

2. Referenced Documents

Installation Procedures (IP) for SATAN version 1.0.0.2, 18 July 1997.

3. Operating Guidelines

The default behavior of this software is to run through Netscape when the SATAN icon is selected.

The configuration variables and command line options can be found in Appendix A.

For the configuration variables, make changes within the /h/COE/Comp/SATAN/bin/SATAN.dir/config/satan.cf file. The command line options must be added at the root prompt like the example below:

/h/COE/Comp/SATAN/bin/SATAN.dir/satan -v

4. Installation Overview

This version of SATAN can be installed in accordance with the Installation Procedures document for SATAN version 1.0.0.2.

5. System Administration Utilities

None.

6. Operation/Maintenance Procedures

None.

7. Error Recovery Guidelines

To shutdown the satan process, type ps -ef at the root prompt to list all of the current processes. Locate the satan process and its process number. Once you have located that number, execute the following:

```
# kill -9 <process number>
```

This will immediately kill the satan process. To restart satan, select the SATAN icon or execute the following at the root prompt:

```
# /h/COE/Comp/SATAN/bin/SATAN.dir/satan
```

If satan will not start, make sure that the first line in the satan file is calling the correct perl script. It should read:

```
#!/bin/perl
```

If that is not correct, you need to make the correction.

Please note that there are other command line options that can be chosen instead of "-v" in Appendix A.

8. Notes

None.

A. Appendices

SATAN satan.8 file. This file is in nroff -man format and is located in /h/COE/Comp/SATAN/bin/SATAN.dir.

satan - network security scanner

SYNOPSIS

satan [options] [primary target(s)...]

DESCRIPTION

SATAN (Security Administrator Tool for Analyzing Networks) remotely probes systems via the network and stores its findings in a database. The results can be viewed with any Level 2 HTML browser that supports the http protocol (e.g. Mosaic, Netscape, etc.)

When no primary target(s) are specified on the command line, SATAN starts up in interactive mode and takes commands from the HTML user interface.

When primary target(s) are specified on the command line, SATAN collects data from the named hosts, and, possibly, from hosts that it discovers while probing a primary host. A primary target can be a host name, a host address, or a network number. In the latter case, SATAN collects data from each host in the named network.

SATAN can generate reports of hosts by type, service, vulnerability and by trust relationship. In addition, it offers tutorials that explain the nature of vulnerabilities and how they can be eliminated.

By default, the behavior of SATAN is controlled by a configuration file (config/satan.cf). The defaults can be overruled via command-line options or via buttons etc. in the HTML user interface.

Options:

-a Attack level (0=light, 1=normal, 2=heavy). At level 0, SATAN collects information about RPC services and from the DNS. At level 1, SATAN collects banners of well-known services such as telnet, smtp and ftp, and can usually establish the type of operating system. At level 2, SATAN does a more extensive (but still non-intrusive) scan for services. Level 2 scans may result in console error messages.

-A proximity_descent

While SATAN extracts information from primary targets, it may discover other hosts. The proximity descent controls by how much the atttack level decreases when SATAN goes from primary targets to secondary ones, and so on. The -z option determines what happens when the attack level reaches zero.

-c 'name=value; name=value...'
Change the value of arbitrary SATAN variables. Example:

-c 'dont_use_dns = 1; dont_use_nslookup = 1'.

The -c option allows you to control configuration and other variables that do not have their own command-line option. The format is a list of name=value pairs separated by semicolons. Variable names have no dollar prefix, and values are not quoted. Whitespace within values is preserved.

-d database
Specifies the name of the database to read from and to save to (default satan__data).

When multiple SATAN processes are run in parallel, each process should be given its own database (for example, one database per subnet of 256 hosts). Use the merge facility of the HTML user interface to merge data from different runs.

-i Ignore the contents of the database.

-l proximity
Maximal proximity level. Primary targets have proximity 0, hosts discovered while scanning primaries have proximity level 1, and so on. SATAN ignores all hosts that exceed the maximal proximity level.

-o only_attack_these
A list of domain names and/or network numbers of hosts that SATAN is permitted to scan. List elements are separated by whitespace or commas. Understands the * shell-like wildcard.

-O dont_attack_these
A list of domain names and/or network numbers that SATAN should stay away from. The list has the same format as with the -o option.

-s Subnet expansion. For each primary target, SATAN finds all alive hosts in the target's subnet (a block of 256 addresses).

-S status_file
While collecting data, SATAN maintains a status file with the last action taken. The default status file is status_file.

-t level
Timeout level (0 = short, 1 = medium, 2 = long) for each probe.

-u Specifies that SATAN is being run from an untrusted host. Access via, for example, the remote shell or network file system services, means that there is a security problem.

-U Opposite of the -u option. SATAN may be run from a possibly trusted host. Access via, for example, the remote shell or network file system services is not necessarily a problem.

-v Verbose mode. SATAN prints on the standard output what it is doing. This is useful for debugging purposes.

-V SATAN prints its version number and terminates.

-z When scanning non-primary hosts, continue with attack level of zero when the level would become negative. The scan continues until the maximal proximity level is reached.

-Z Opposite of the -z option.

FILES
config/* configuration files
rules/* rule bases
results/* data bases

AUTHORS
Dan Farmer, Wietse Venema

This page intentionally left blank.